Amendments to the Claims:

1. (currently amended) A computer implemented method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

accessing said computer usable password policy data structure by a password policy enforcement agent; ~~and~~

enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent;

determining a strength of one of said plurality of password policies based on said enforcing; and

dynamically modifying one of said plurality of password policies based on said strength.

2. (currently amended) The computer implemented method of Claim 1 wherein said computer usable password policy data structure comprises a file structure compatible with extensible markup language.

3. (currently amended) The computer implemented method of Claim 1 wherein said password policy enforcement agent is operable on a client computer of a client-server computer system.

4. (currently amended) The computer implemented method of Claim 1 wherein said method is operable on a utility data center.

5. (currently amended) The computer implemented method of Claim 1 further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent.

6. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account.

7. (currently amended) The computer implemented method of Claim 6 wherein said plurality of password policies comprises a parameter indicating a time duration, and wherein exceeding said threshold parameter triggers locking of a computer system access account within said time duration.

8. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt.

9. (currently amended) The computer implemented method of Claim 8 wherein access to said computer system access account is delayed for an increasing time period for successive unsuccessful access attempts.

10. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a minimum password length parameter.

11. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a maximum password length parameter.

12. (currently amended) The computer implemented method of Claim ~~12~~ wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a word associated with a natural language.

13. (currently amended) The computer implemented method of Claim 12 wherein said natural language is English.

14. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a palindrome.

15. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a derivative of a computer system account name.

16. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a password.

17. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a pronounceable password consistent with said plurality of password policies.

18. (currently amended) The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for specifying a set of characters utilizable to automatically generate a password.

19. (currently amended) The computer implemented method of Claim 1 further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about whether said at least one of said plurality of password policies has been successfully enforced.

20. (currently amended) Instructions on a computer usable storage medium wherein the instructions when executed cause a computer system to perform a method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

providing an access point with access to said computer usable password policy data structure; ~~and~~

receiving feedback from a password policy enforcement agent associated with said access point about which of said plurality of password policies have been successfully enforced;

determining a strength of one of said plurality of password policies based on said feedback; and

dynamically modifying one of said plurality of password policies based on said strength.

21. (currently amended) The computer usable storage medium of Claim 20 wherein said computer usable password policy data structure comprises a file structure-compatible with extensible markup language.

22. (currently amended) The computer usable storage medium of Claim 20 wherein said method further comprises:

selecting a computer access password policy parameter from said plurality of computer access password policy parameters consisting of a parameter selected from a group of parameters comprising a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account, a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account, an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt, a minimum password length parameter, a maximum password length parameter, a parameter to prohibit passwords consisting of a natural language word, a parameter to prohibit passwords consisting of a palindrome, a parameter to prohibit passwords consisting of a derivative of a computer system account name, a parameter to automatically generate a password, a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies, and a parameter to specify a set of characters utilizable to automatically generate a password.

23-24 (cancelled)